IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	Civil No. 1:14-cv- 1273
v.	)	
	)	**FILED *EX PARTE* AND UNDER SEAL**[1]
HAMMAD AKBAR,	)	
	)	
Defendant.	)	
	)	

UNITED STATES' MEMORANDUM OF LAW IN SUPPORT OF MOTION FOR TEMPORARY RESTRAINING ORDER

Plaintiff, the United States of America, by and through its attorneys, pursuant to 18 U.S.C. § 2521 and Federal Rule of Civil Procedure 65, hereby seeks an *ex parte* temporary restraining order commanding the defendant to halt the marketing, sale, and advertising of a mobile spyware application ("app") that surreptitiously intercepts a variety of both outgoing and incoming wire and electronic transmissions to and from the smartphone on which it is installed. The United States further requests that the order prohibit the Defendant's agents, servants, employees, and all persons and entities in active concert or participation with him, from engaging in any of the activity described in the United States' complaint in this matter, or from causing any of the injury described in the United States' complaint, and from assisting, aiding, or abetting any other person or business entity from engaging in or performing any of the activity described in the United States' complaint

[1] This filing is accompanied by a Motion to Seal and a Memorandum in Support, as required by Local Civil Rule 5(D).

I. OVERVIEW

Defendant operates the company that markets, sells, and advertises the StealthGenie app, and is the leader of the criminal conspiracy responsible for StealthGenie. The app is marketed, advertised, and sold via a website hosted on a computer server located in the Eastern District of Virginia. The communications surreptitiously intercepted by StealthGenie are stored on an online portal hosted on a computer server also located in the Eastern District of Virginia. The website and online portal are accessed through a domain name, stealthgenie.com.

Defendant is causing continuing and substantial injury in this District, in the United States, and around the world to unknowing smartphone users whose communications are being surreptitiously intercepted by StealthGenie. In this action, the United States seeks injunctive relief commanding Defendant to stop marketing, selling, and advertising StealthGenie. To give effect to this prohibition, the United States further seeks an Order: (1) directing Amazon Web Services, Inc. to the restrain and lock the relevant account associated with StealthGenie to take all information associated with the account offline; and, (2) requiring Verisign, Inc., to restrain and lock domain stealthgenie.com, which would block connection attempts to the StealthGenie website and its associated online portal.

II. BACKGROUND

The FBI has been engaged in a multi-year investigation of the marketing, advertising, and sale of a mobile spyware application ("app") that illegally intercepts wire and electronic communications made using smartphones. This app is marketed as "StealthGenie." *See* Declaration of Special Agent Sarah E. Jones ("Jones Decl.") at ¶4. Hammad Akbar operates the

company that markets, sells, and advertises the StealthGenie app, InvoCode Ltd ("InvoCode"). *Id.*

A. Marketing and advertisement of StealthGenie

While reviewing available spyware applications on the Internet from a location within the Eastern District of Virginia on November 5, 2011, FBI Special Agent Matthew Murray observed advertisements for StealthGenie, available at www.stealthgenie.com (hereinafter "StealthGenie website"). *Id.* at ¶5. Agent Murray captured the content of the StealthGenie website on that date, which Special Agent Sarah E. Jones later reviewed. *Id.*

The StealthGenie website stated that the app was designed to run on a variety of mobile smartphone platforms, including Google Inc.'s Android platform, Blackberry Limited's Blackberry platform, and Apple Inc.'s iPhone platform. *Id.* at ¶6. It advertised the app as being covert in nature and running behind the scenes without the knowledge of the user. *Id.* at ¶7. The website specifically touted StealthGenie as "100% undetectable" and promised the ability to monitor phones "without worry of being caught." *Id.*

The StealthGenie website stated that the app had numerous functionalities that permitted it to intercept a variety of both outgoing and incoming wire and electronic transmissions to and from the smartphone on which it was installed. *Id.* at ¶8. These functionalities included the interception of the following types of wire and electronic communications:

- Call Recording: Records all incoming/outgoing voice calls or those specified by the purchaser of the app (hereinafter "purchaser");
- Call Interception: Allows the purchaser to intercept calls on the phone to be monitored while they take place, without the knowledge of the monitored smartphone user (hereinafter "user");

- Recorded Surroundings: Allows the purchaser to call the phone and activate it at any time to monitor all surrounding conversations within a fifteen (15)-foot radius without the knowledge of the user;
- Electronic Mail: Allows the purchaser to monitor the incoming and outgoing e-mail messages of user, read their saved drafts, and view attachments;
- SMS: Allows the purchaser to monitor the user's incoming and outgoing SMS messages;
- Voicemail: Allows the purchaser to monitor incoming voicemail messages;
- Contacts: Allows the purchaser to monitor the entries in the user's address book;
- Photos: Allows the purchaser to monitor the photos on the user's phone;
- Videos: Allows the purchaser to monitor the videos on the user's phone; and
- Appointments: Allows the purchaser to monitor the user's calendar entries.

Id.

According to the website, all data gathered by the app was uploaded to a "Member's Area," where the purchaser can remotely access the information from any Internet-capable device. *Id.* at ¶9. The website stated that "the whole process of download and activat[ing]" the StealthGenie app would take "less than 1 minute." *Id.* According to the website, the purchaser "will only need to have the phone in [their] hand for a very short period of time and will never need to access it again" and "will be able to view and control all the activities on the phone remotely from [their] secure Stealthgenie member area." *Id.*

The website specifically described scenarios for use of the app where the purchaser did not have a possessory interest in the monitored phone. *Id.* at ¶10. For example, in an answer to the "frequently asked question" of , "Will the target users ever find out that this application is running in their cell phones?," the website stated, "No, the target phone users will never be able to find out that this application has been installed in their phones. This is highly undetectable

application which works in the background without even letting the user know that something is running in their phones. When it is successfully installed you receive a prompt message saying 'StealthGenie started successfully'." *Id.*

The website included several purported testimonials of interest describing scenarios for use of the app where the purchaser did not have a possessory interest in the monitored phone. *Id.* at ¶11. It also included a section entitled, "Catch Cheating Spouse." *Id.* This section was accessed by clicking a "Buy Now" button accompanying a graphic stating, "Suspect your spouse is cheating? Put an end to the speculation and suspicious behavior. You deserve to know if you are being lied to. Know the truth about whether or not your spouse is cheating." *Id.* In pertinent part, the accompanying text stated, "StealthGenie is a mobile spy software that can help you find out what your husband, wife, boyfriend or perhaps your girlfriend are hiding from you. You can monitor them without getting suspected because once installed, StealthGenie is completely undetectable and operates mutely without interrupting the calls or other cellular functions." *Id.*

In apparent contradiction of these testimonials and claims, on a page entitled "Disclaimers," the website stated: "Our software is designed for monitoring your children or employees on a smartphone you own or have proper consent to monitor. You must notify users of the smartphone that they are being monitored. Failure to do so may result in the breaking of federal and state laws. If you install software onto a device of which you do not own or have proper consent, we will cooperate with law officials to the fullest extent possible." *Id.* at ¶12.

The StealthGenie website was hosted at a U.S.-based provider, Amazon Web Services, Inc. (hereinafter "AWS"). AWS provides web hosting services in the United States, including at a data center located in Ashburn, Virginia, which is in the Eastern District of Virginia. *Id.* at ¶13.

Agent Jones conducted another live capture of the website on February 15, 2013. *Id.* at ¶14. The website as of that date no longer had the "Catch Cheating Spouse" page or most of the testimonials from purported individuals who were monitoring spouses, romantic partners, and adult children. *Id.* However, even on February 15, 2013, the StealthGenie website still contained language emphasizing the surreptitious nature of the software. *Id.* at ¶15. The website stated that the app "is completely safe to use as the target user can never find out that they are being monitored." *Id.* Further, under the section "How StealthGenie Works," the website stated:

> Keeping an eye on someone seems to be a painstakingly hard job, doesn't it? If you wanted to monitor someone, you would most probably do one of the following things:
>
> - Splurge on expensive surveillance equipment
> - Hire a costly private investigator
> - Follow them around
> - Go through their stuff
> - Interrogate their friends
>
> But you know these methods would cost too much and take too long with no guarantee of results...
>
> Or you could just grab their cell phone and go through it as you know that their phone is the most likely place to find all the information you need.
>
> But you know that's practically impossible to do.
>
> Well, not anymore. With StealthGenie, the most powerful cell phone spy software, you could be monitoring their phone remotely and invisibly, within minutes and at the cost of a cup of coffee a day!

Id.

The February 15, 2013, website also had several frequently asked questions of interest:

> ["]Will monitored phone user know StealthGenie is installed on their phone?["]
>
> StealthGenie works completely invisibly so the monitored phone user will not be able to see the name 'StealthGenie' (or anything similar) anywhere on their phone.
>
> ["]I am worried they monitored phone user will find out I am monitoring them?["]
>
> You don't have to worry about the monitored user finding StealthGenie on their phone as the application works in stealth mode and is not detectable at all.

Id. at ¶16.

As of September 22, 2014, the StealthGenie website still offered the StealthGenie app for sale. *Id.* at ¶17. It was also still hosted at AWS, at its data center located in Ashburn, Virginia. *Id.*

B. Sale and testing of StealthGenie

On December 14, 2012, Agent Jones purchased the Android version of the StealthGenie app. *Id.* at ¶18. The various functionalities of the app were then tested on December 17, 2012, in the Eastern District of Virginia. *Id.* Prior to testing, Agent Jones established an account in StealthGenie's "Member's Area" (hereinafter "online portal") to permit her to determine the data from the phone that had been collected by the app. *Id.* at ¶19. During testing, agents assisting Agent Jones were logged-on to the online portal, located at cp.stealthegenie.com/services, to review data. *Id.*

In pertinent part, the online portal listed the following type of potentially collected information for review: "Call Logs," "Recorded Calls," "SMS Logs," "Recorded Surroundings," "Gmail," "E-mail," "Contacts," "Appointments," "Photos," "Videos," and "Music." *Id.* at ¶20. Review of the portal revealed that the app successfully intercepted wire and electronic

communications during testing of the phone, including call logs, SMS logs, "recorded surroundings," contacts, appointments, and photos. *Id.*

While logged into the online portal, data captured in near real-time was presented on multiple occasions. *Id.* at ¶21. When a text or phone call was placed from the target phone, a window appeared on the website dashboard notifying the web user of the target phone activity. *Id.* In addition, agents received an alert e-mail in near real time each time a text was sent from the target phone to a target phone number (this functionality was set up in a settings portion of the online portal). *Id.* As of September 22, 2014, the online portal was also hosted at AWS, at its data center located in Ashburn, Virginia. *Id.* at ¶22. The online portal at subdomain cp.stealthgenie.com allowed user log-in on September 22, 2014. *Id.*

C. Technical analysis

FBI agents obtained a search warrant to seize the StealthGenie website and associated data from AWS, including the data from the online portal. *Id.* at ¶23. The data returned by AWS reflected the state of stealthgenie.com as of December 19, 2011. *Id.* Review of the data by the FBI's Investigative Analysis Unit ("IAU") revealed that as of that time period, the outward-facing website content looked substantively identical to that observed on November 5, 2011. *Id.*

IAU's analysis concluded that StealthGenie was a smartphone spyware application with a minimal footprint which made it difficult to detect for a non-technical user. *Id.* at ¶24. Like many other such applications, StealthGenie was able to record SMS and phone conversations, capture photographs, videos, and stored music, as well as contact lists, calendars and other data. *Id.* Unlike most other vendors' products, StealthGenie allowed the service's subscribers to create

triggers to both selectively capture most types of data as well as to alert the subscriber of specific actions that occur on the smartphone. *Id.*

IAU determined that in order to install the app, the purchaser needed at least temporary possession of the target phone. *Id.* at ¶25. During the installation process on an Android smartphone, the person installing the app must affirmatively grant a series of permissions that allow the application to access privileged information. *Id.* Once the program was activated it was started as a "background" (i.e., hidden) service and set up to launch, automatically, when the phone was powered on. *Id.* The only time that the application interacted with the screen was during activation. *Id.* The icon for the application was removed from the menu making it unlikely that an unsophisticated user would know that it had been installed. *Id.*

IAU found that the HTTP (i.e., web) protocol was used by the app to upload data and media to the StealthGenie server. *Id.* at ¶26. Most events were not directly uploaded; instead, they were saved to local databases which were created on the phone, or copied from log data or other data recorded by specific application, such as the phone's contact list. *Id.* The StealthGenie app kept a record of changes both on the server (e.g., subscriber preferences) and the phone itself. *Id.* at ¶27. When changes were made a virtual flag was set to indicate that data was no longer correctly synchronized between the phone and the StealthGenie server. *Id.*

On the phone, the StealthGenie application operated in one of two modes. *Id.* at ¶28. "ACTIVE" mode meant that the phone was connected to the Internet (mobile data or wi-fi), whereas "PASSIVE" mode meant that it was not connected to the Internet at all. *Id.* Database synchronization and media uploads were understandably performed only in ACTIVE mode. *Id.* Because database synchronization generally occurred quickly when the phone was in ACTIVE

mode, notifications could occur in close to real-time when the phone was connected to the Internet. *Id.*

Triggers were an advanced feature of StealthGenie compared to competitors' products. *Id.* at ¶29. A trigger is an event which results in an immediate response, for example, a call made to or received from a specific phone number. *Id.* The subscriber had the option to be notified when a trigger was fired either by SMS or e-mail. *Id.* Triggers could also include specific words or phrases found in SMS texts or e-mails. *Id.* When a trigger was initiated, a command was transmitted from the target phone to the StealthGenie server, which would ten transmit the SMS or e-mail alert. *Id.* Notably, these alerts did not contain the content of the communication concerning the event (i.e., a user would be alerted to a text being received, but would not be provide the content of the text, which would need to be viewed via the online portal). *Id.*

IAU's analysis determined that StealthGenie was capable of performing most of the functionalities advertised. *Id.* at ¶30. This includes several functionalities that were not confirmed via agent testing, including monitoring telephone calls, live call interception, monitoring voicemail, recorded surroundings, and, videos. *Id.* IAU determined from review of user data the vast majority of targets of StealthGenie monitoring were adult friends and relatives. *Id.* In many cases it seemed clear that the intended purpose of the monitoring was to detect suspected infidelity. *Id.*

III. DEFENDANT

According to "whois" information, the domain stealthgenie.com was originally registered to InvoCode, located at 199 School Road, Hall Green, Birmingham, B28 8PE, UNITED KINGDOM. *Id.* at ¶31. The administrative contact was Hammad Akbar, with an e-mail address

of hammad2707@gmail.com. *Id.* On February 13, 2012, the "whois" record for the domain was put into identity protection where it has remained since then, although the registrar has changed. *Id.*

According to IAU's analysis of stealthgenie.com, logs indicated that Hammad Akbar was one of the most frequent users of StealthGenie's administrator login. *Id.* at ¶32. The StealthGenie user database contained multiple accounts for Akbar, most likely for testing purposes. *Id.* E-mails found in the StealthGenie database imply that Akbar tested a number of competitors' products, including eBlaster, Mobistealth, and Mobile Spy. *Id.* A huge majority of the administrative logins to StealthGenie occurred from IP addresses located in Lahore, PAKISTAN, where Akbar is believed to reside, along with his employees. *Id.*

InvoCode had a public website, invocode.com. *Id.* at ¶33. InvoCode's website advertised itself as providing "GPS based tracking solutions." *Id.* The website further stated, "[W]ith our state-of-the-art tracking products you can track the location of your employees. Geo Fence their movement and monitor their activities." *Id.* The website provided two contact addresses: 199 School Road, Hall Green, Birmingham, B28 8PE, UNITED KINGDOM (i.e., the address from whois information), and 48 D-1a Gulberg III, off MM Alam Road, Lahore, 54660, PAKISTAN. *Id.*

Open-source research indicated that Akbar possessed a public listing on the social networking website LinkedIn. *Id.* at ¶34. Akbar's profile stated that he was the CEO of InvoCode, located in West Midlands, UNITED KINGDOM. *Id.* His profile stated that he had "been through the process of moving from UK to south Asia to setup and bootstrap a mobile applications development company." *Id.* His profile stated that InvoCode had 11-50 employees

and had been in existence from November 2011. *Id.* Akbar was also the CEO of InvoCube, which was created in January 2012 and is the "Mobile Gaming division" of InvoCode. *Id.*

The FBI's undercover buy of the StealthGenie app required payment by PayPal. *Id.* at ¶35. Records revealed that several PayPal accounts had been established by Akbar, including one under the accountholder name StealthGenie and another under the name InvoCode. *Id.* The purchase made by the FBI could not be linked to the records received.

A response by AWS to compelled process indicated that the account associated with the stealthgenie.com domain belonged to subscriber Cubitum Limited, located at Unit 1010, Miramar Tower 132, Nathan Road, TSIM SHA TSUI, Hong Kong, CHINA. *Id.* at ¶36. The billing contact was Hammad Akbar, at the same address. *Id.*

As noted above, the registration e-mail address associated with the StealthGenie domain was hammad2707@gmail.com. *Id.* at ¶37. A search warrant was obtained for this account on December 9, 2011. *Id.* The registrant of the account was Hammad Akbar. *Id.* Various e-mails found in this e-mail account demonstrate Akbar's leadership role in directing the marketing, advertisement, and sale to StealthGenie. *Id.* at ¶38. E-mails in the account also indicated that the primary target market for the app was the "Spousal Cheat" market. *Id.*

Akbar was indicted in the Eastern District of Virginia on August 7, 2014, for violations of 18 U.S.C. §§ 371 (conspiracy), 2512(1)(b) (sale of an interception device), 2512(1)(c)(i) (advertisement of a known interception device), and 2512(1)(c)(ii) (advertising a device as an interception device) arising from his leadership role in the marketing, advertising, and sale of StealthGenie. The indictment against Akbar is currently under seal, but will be unsealed on September 29, 2014, if the Court grants the TRO sought by the Government.

IV. STEALTHGENIE HARMED VICTIMS IN THIS DISTRICT, THROUGHOUT THE UNITED STATES, AND WORLDWIDE

StealthGenie has caused enormous injury in this District and throughout the United States. As of December 19, 2011, the date of the user data analyzed by IAU, hundreds of users around the United States and worldwide had been collected by the application. *Id.* at ¶30. The product has been marketed and sale for almost three years since the date of the user data analyzed by IAU, leading to the fair inference that thousands, if not tens of thousands, of users worldwide have had their most personal and private communications improperly intercepted by StealthGenie.[2]

Moreover, the product has been advertised and sold in this District, as demonstrated by Agent Jones's undercover purchase. During the testing of the product, wire and electronic communications were intercepted in this district. Indeed, because the StealthGenie website remains functional, the app is being advertised in this district at present.

Akbar's conduct in the marketing, advertising, and sale of StealthGenie represents a quintessential invasion of privacy of victim smartphone users. As Congress noted in enacting section 2512:

> Virtually all concede that the use of wiretapping or electronic surveillance techniques by private unauthorized hands has little justification where communications are intercepted without the consent of one of the participants. . . . It is not enough, however, just to prohibit the unjustifiable interception, disclosure, or use of any wire or oral communications. An attach must also be made on the possession, distribution, manufacture and advertising of intercepting devices. All too often the invasion of privacy itself will go unknown. Only by

[2] Investigations involving serious invasions of privacy, like that undertaken in the instant case, require the making of delicate judgment calls. The Government seized and reviewed the database of user communications intercepted by StealthGenie through December 2011 in order to build its criminal case. As the information collected was more than sufficient, the Government decided that seeking subsequent warrants simply to determine the extent of the expansion of StealthGenie's user base would be unduly intrusive, under the circumstances.

> striking at all aspects of the problem can privacy be adequately protected. The prohibition, too, must be enforced will all appropriate sanctions. Criminal penalties have their part to play. But other remedies must be afforded the victim of an unlawful invasion of privacy. Provision must be made for civil recourse for dangers. The perpetrator must be denied the fruits of his unlawful actions in civil and criminal proceedings.

S.Rep. No. 1097 90th Congress, 2d Session, reprinted in 1968 U.S.C.C.A.N. 2112, 2156.

V. THE UNITED STATES NEEDS JUDICIAL INTERVENTION TO DISABLE STEALTHGENIE

The United States proposes a comprehensive plan to disable StealthGenie. Jones Decl. at ¶39. The first step toward towards stopping the marketing, advertising, and sale of StealthGenie is the restraint and locking of the relevant account(s) at AWS. *Id.* at ¶40. The TRO sought as part of this action seeks an order to AWS that would direct it take all information associated with the account(s) offline. *Id.* This would include the StealthGenie website and its associated online portal. *Id.* The order would also make the account inaccessible to Defendant. *Id.*

The second step toward towards stopping the marketing, advertising, and sale of StealthGenie is to end the operation of the domain stealthgenie.com. *Id.* at ¶41. This domain is controlled by a registry in the Eastern District of Virginia, Verisign, Inc., located at 12061 Bluemont Way, Reston, Virginia 20190. *Id.* The TRO sought as part of this action seeks an order to Verisign, Inc. requiring it to lock and make inaccessible the domain stealthgenie.com, which would block connection attempts to the StealthGenie website and its associated online portal. *Id.*

VI. ARGUMENT

A. Jurisdiction and Venue Are Proper in This Court

Section 2521 of Title 18 authorizes the United States to "commence a civil action in any Federal court" to enjoin fraud, and to "initiate a civil action in a district court of the United States" to enjoin illegal interception of communications. As detailed above, and in the Complaint filed herewith, Defendant has, and continues to, market, advertise, and sell StealthGenie in this District. Likewise, Defendant's agents, and persons and entities who are in active concert and participation with him, continue to participate in the marketing, advertising, and sale of StealthGenie in this District. Accordingly, subject matter jurisdiction is proper in this Court. This Court may also exercise personal jurisdiction over Defendant, who is a foreign national who has deliberately targeted victims in this District. Venue is proper under 28 U.S.C. § 1391(b)(2), for the reasons discussed below in relation to personal jurisdiction.

At the complaint stage, a *prima facie* case by the plaintiff of personal jurisdiction is sufficient. *Eurofins Pharma US Holdings v. BioAlliance Pharma SA*, 623 F.3d 147, 155 (3d Cir. 2010). For claims arising under federal law, serving a summons or filing a waiver of service establishes personal jurisdiction over a defendant who is subject to the jurisdiction of a court of general jurisdiction in the state where the district court is located. Fed. R. Civ. P. 4(k)(1); *see Provident Nat'l Bank v. California Federal Sav. & Loan Ass'n*, 819 F.2d 434, 437 (3d Cir. 1987) ("A federal district court may assert personal jurisdiction over a nonresident of the state in which the court sits to the extent authorized by the law of that state."). Virginia's long-arm statute extends personal jurisdiction to the limits allowed by the Due Process Clause. *Consulting Eng'rs Corp. v. Geometric Ltd.*, 561 F.3d 273, 277 (4th Cir. 2009).

Pursuant to the Virginia long-arm statute, this Court may assert personal jurisdiction if the defendants have sufficient "minimum contacts" with this forum and if subjecting the defendants to the court's jurisdiction comports with "traditional notions of fair play and substantial justice." *International Shoe Co. v. Washington*, 326 U.S. 310, 316-17 (1945). Where, as here, the cause of action is related to the defendant's contacts with the forum, it is sufficient if the contacts show "purposeful availment" by the defendant of an opportunity to conduct activity in the forum state. *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 475 (1985) ("Jurisdiction is proper . . . where the contacts proximately result from actions by the defendant *himself* that create a "substantial connection" with the forum).

Defendant's victims include smartphone users in Virginia. Defendant also advertised and sold StealthGenie in Virginia. Accordingly, Defendant's conduct readily satisfies the "minimum contacts" requirement of due process, and personal jurisdiction is consistent with the Virginia long-arm statute.

B. The United States is Entitled to Preliminary Injunctive Relief

Generally, in this Circuit, a party requesting injunctive relief must establish: (1) a clear showing that it will succeed on the merits; (2) a clear showing that it is likely to be irreparably harmed absent preliminary relief; (3) the balance of equities tips in favor of the moving party; and (4) a preliminary injunction is in the public interest. *Real Truth About Obama, Inc. v. Fed. Election Comm.*, 575 F.3d 342, 346-47 (4th Cir. 2009). However, where, as here, the United States seeks an injunction pursuant to federal statutes enacted to protect the public interest that provide for injunctive relief, the Court is authorized to issue the injunction if the statutory conditions are satisfied. *See Rum Creek Coal Sales, Inc. v. Caperton,* 926 F.2d 353, 362, n. 12

(4th Cir.1992) (noting that "courts have found the irreparable harm requirement unnecessary where an injunction is authorized by a federal statute"); *see also United States v. Nutrition Serv., Inc.*, 227 F. Supp. 375, 388–89 (W.D. Pa. 1964), *aff'd* 347 F.2d 233 (3d Cir. 1965) ("There is sufficient showing [for an injunction], where, as here, the Government presents evidence of violations of the provisions of a statute enacted for the protection of the public. . . . Nor is it necessary to demonstrate the precise way in which violations of the law might result in injury to the public interest. It is sufficient to show only that the threatened act is within the declared prohibition of Congress.").

The statute at issue here clearly authorizes injunctive relief. The United States may obtain an injunction against illegal interception of communications in violation of 18 U.S.C. §§ 2511 and 2512:

> Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought.

18 U.S.C. § 2521.

The relevant inquiry, therefore, focuses on whether the United States has met its burden of showing that injunctive relief is necessary to prevent the violation of the statute at issue – 18 U.S.C. § 2512. As described below, the United States has more than met this burden, and urges the Court to prevent the Defendant, its agents, and those acting in concert, from persisting in their illegal activity.

C. The Court Should Issue an Order Preventing Defendant from Selling, Marketing, and Advertising a Product that is Surreptitiously and Illegally Intercepting Electronic Communications

As detailed in Special Agent Jones's Declaration, and summarized above, the Defendant is marketing, selling, and advertising a mobile spyware application that surreptitiously intercepts a variety of both outgoing and incoming wire and electronic transmissions to and from the smartphone on which it is installed. The United States is therefore fully authorized to obtain an injunction under 18 U.S.C. § 2521. The United States has met its burden to demonstrate the necessity for injunctive relief under § 2521. Special Agent Jones's Declaration demonstrates that the United States easily meets its burden of proof regardless of which evidentiary standard is applied. It is a violation of the Wiretap Act when one:

> manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or
>
> [] places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of –
>
> > (i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
> >
> > (ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications,
>
> knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce . . . .

18 U.S.C. §§ 2512(1)(b), (c)(1), (c)(2).

As Special Agent Jones's Declaration indicates, Akbar marketed, sold, and advertised StealthGenie, which surreptitiously intercepts a variety of both outgoing and incoming wire and electronic transmissions to and from the smartphone on which it is installed. This conduct clearly violates 18 U.S.C. §§ 2512(1)(b), (c)(1), and (c)(2). As such, the Court should grant injunctive relief to prevent this conduct, pursuant to 18 U.S.C. § 2521.

D. To Prevent the Unlawful Conduct being Perpetrated by the Defendant and StealthGenie, the Court Should Issue an Order that Appropriately Restricts AWS and Verisign from Engaging in certain Conduct related to StealthGenie

As described in more detail above, the TRO sought by the Government would: (1) direct AWS to the restrain and lock the relevant account(s) associated with StealthGenie to take all information associated with the account offline; and (2) require Verisign, Inc., to restrain and lock domain stealthgenie.com, which would block connection attempts to the StealthGenie website and its associated online portal. By ordering this relief, the Court will halt Defendant's advertisement and sale of StealthGenie, a product used to wiretap U.S. citizens.

The relief the United States seeks here is authorized by Fed. R. Civ. P. 65, which provides that a preliminary injunctive relief, including a temporary restraining order, may bind:

> (C) the parties' officers, agents, servants, employees, and attorneys; and
> (D) other persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B)

Fed. R. Civ. P. 65(d)(2).

An injunction alone against the defendant will not prevent the ongoing crime. To avoid that untenable outcome, it is submitted that the district court is to ensure that all parties involved in the illegal process be held accountable to the court should they elect to play any role in

allowing the unlawful sale or use to continue. The connection between AWS and Verisign is more than circumstantial or incidental. The relationship is an intentional, commercial for-profit relationship. AWS and Verisign, must be considered either "agents" of the Defendant, or persons or entities "who are active in concert or participation" with the Defendant. Based upon the facts of this case as described in the attached declaration, which show that both AWS and Verisign are instrumental and necessary in the sales and distribution of the illegal service the Defendant provides, both AWS and Verisign fall under the purview of those who could be considered "agents" of the Defendant, or those who are "acting in concert" with the Defendant to provide illegal material. Fed. R. Civ. P. 65(d)(2) & (3). The Federal Circuit has defined a person who is in "active concert or participation" with an enjoined party, and thus bound by the injunction, if 'he aids or abets an enjoined party in violating [the] injunction,' or if he is in privity with an enjoined party." *Blockowicz v. Williams*, 630 F.3d 563, 567 (Fed. Cir. 2010). AWS and Verisign are both aiding and abetting the Defendant, and are in contractual privity with him. They are clearly are in active concert or participation with the Defendant, and are subject to the order the United States requests here. *See Avoe Corp. v. AE TECH CO., LTD., et al.*, 727 F.3d 1375, 1384 (holding that preliminary relief may be granted against non-party entity who acted as a distributor for infringing product).

It is worth noting that district courts generally have broad discretion in deciding whether to grant injunctive relief. *See General Instrument Corp. of Delaware v. Nu-Tek Elecs.& Mfg., Inc.*, 197 F.3d 83, 90 (3d Cir. 1999). As courts of equity, district courts "'may, and frequently do, go much farther both to give and withhold relief in furtherance of the public interest than they are accustomed to go when only private interests are involved.' . . . This is especially the case

where the public interest in question has been formalized in a statute." *Instant Air Freight Co. v. C.F. Air Freight, Inc.*, 882 F.2d 797, 803 (3d Cir. 1989) (quoting *Virginian Ry. Co. v. System Fed'n No. 40*, 300 U.S. 515, 552 (1937)).

Section 2521 of Title 18 enhances the Court's traditional powers at equity by allowing the Court to promptly enjoin ongoing fraudulent or unauthorized interception upon a suit by the Government. Section 2521 confers broad authorization for courts to enter restraining orders "at any time," or to "take such other action, as is warranted to prevent a continuing and substantial injury." 18 U.S.C. § 2521.

Civil injunctive relief, such as that sought in this application, has been used in several districts to accomplish large-scale disruptions of widespread computer hacking. In some cases, the United States Government has been the plaintiff, and in others, a private party has sought the injunctions. In all cases, injunctions have enabled the plaintiffs to halt hackers' schemes without infringing upon the privacy or property interests of victims or other parties. For example, courts, including this District, have entered preliminary injunctive relief granting relief more extensive than the relief sought here. *See, e.g., Microsoft Corp. v. John Doe*, No. 1:13-cv-139, 2014 U.S. Dist. LEXIS 48398 (E.D. Va. January 6, 2014); and *Microsoft Corp. v. Doe, et al.*, No. 1:10-CV-156, Dkt. No. 27 (E.D. Va. Feb. 22, 2010).

VII. *EX PARTE* RELIEF IS APPROPRIATE

The purpose of a temporary restraining order is to preserve the status quo until the Court has an opportunity to pass on the merits of a preliminary injunction. *See Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers Local No. 70*, 415 U.S. 423, 439 (1974); *Garcia v. Yonkers Sch. Dist.*, 561 F.3d 97, 107 (2d Cir. 2009). A District Court may grant a

temporary restraining order without notice to defendants if "specific facts in an affidavit or verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition," and the movant "certifies in writing any efforts made to give notice and the reasons why it should not be required." Fed. R. Civ. P. 65(b)(1).

The relief sought herein would prevent further unlawful interception of wire and electronic communications. If notified in advance of the Government's intended actions, Akbar could shift his hosting provider and domains, or take other technical steps – which would not require substantial time or effort – to avoid the planned disablement of his operations. The requested *ex parte* relief is necessary to prevent such evasion of the Government's remedial measures. *See* 18 U.S.C. §2521 (the "court shall . . . take such other action as is warrant to prevent a continuing and substantial injury"); Fed. R. Civ. P. 65(b)(1). Therefore, the Court should issue the TRO – without notice to the Akbar or its agents, or those acting in concert with the Defendant – to ensure that the criminal conduct described in the United States' complaint does not continue.

///

///

Conclusion

For the foregoing reasons, the Government respectfully requests the Court grant the relief requested.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: _____

Kevin J. Mikolashek
Jay V. Prabhu
Assistant United States Attorneys
United States Attorney's Office
Counsel for the United States
2100 Jamieson Avenue
Alexandria, VA 22314
Phone: (703) 299-3700
Fax: (703) 299-3981
Email: jay.prabhu@usdoj.gov
Kevin.mikolashek@usdoj.gov

William A. Hall, Jr.
Trial Attorney
Criminal Division, U.S. Department of Justice
1301 New York Ave., NW, Ste. 600
Washington, DC 20530
Phone: (202) 353-4249
Fax: (202) 514-6113
Email: william.a.hall@usdoj.gov